(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 745 924**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 02903**

(51) Int Cl[6] : **G 06 F 1/00**. G 06 F 9/46. 9/30

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 07.03.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 12.09.97 Bulletin 97/37.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CP8 TRANSAC* — FR.

(72) **Inventeur(s) :** UGON MICHEL.

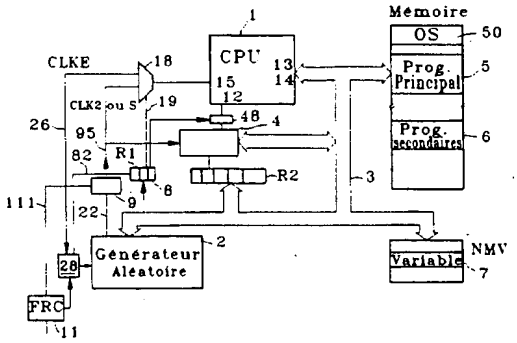
(73) **Titulaire(s) :** .

(74) **Mandataire :** BULL SA.

(54) CIRCUIT INTEGRE PERFECTIONNE ET PROCEDE D'UTILISATION D'UN TEL CIRCUIT INTEGRE.

(57) La présente invention concerne un circuit intégré perfectionné et le procédé d'utilisation d'un tel circuit intégré.

Le circuit intégré perfectionné possède des moyens tant de décorrélation (6. 2. 9. 18. 40) du déroulement d'au moins une séquence d'instruction d'un programme (5) avec les signaux électriques internes ou externes du circuit intégré (1).



FR 2 745 924 - A1

CIRCUIT INTEGRE PERFECTIONNE ET PROCEDE D'UTILISATION D'UN TEL CIRCUIT INTEGRE

La présente invention concerne un circuit intégré perfectionné et le procédé d'utilisation. L'invention trouve son application notamment dans les microprocesseurs ou microcalculateurs et également dans les circuits à logiques câblées nécessitant une sécurisation.

Il est connu que les microprocesseurs ou les microcalculateurs exécutent séquentiellement des instructions successives d'un programme enregistré dans une mémoire, en synchronisme avec un ou plusieurs signaux de cadencement référencés par rapport à un des signaux d'horloge fournis au microprocesseur ou au microcalculateur soit en interne soit en externe.

Il est ainsi possible de corréler les différentes phases de cette exécution de programme avec les signaux d'horloge puisque l'exécution d'une instruction particulière se décompose elle-même en plusieurs étapes cadencées par une ou plusieurs impulsions d'horloge successives. En effet, dans les microprocesseurs de l'art antérieur, le fonctionnement est cadencé régulièrement par les signaux d'horloge provenant en général d'un circuit séquenceur qui engendre les impulsions électriques nécessaires, notamment en déphasant les signaux par rapport à l'horloge de référence. En outre le séquencement des actions doit tenir compte des temps nécessaires pour accéder aux divers registres, aux mémoires et aux organes internes, mais aussi et surtout aux temps de propagation des signaux sur les bus et à travers les divers circuits logiques. Dès lors, les instants de début et de fin de chaque instruction étant parfaitement connus, il est en principe possible de savoir quelle est l'instruction qui s'exécute à un moment

donné dans l'unité de traitement du processeur puisque le programme qui se déroule est constitué d'une suite prédéterminée d'instructions.

On peut, par exemple, déterminer le nombre d'impulsions d'horloge délivrées à partir du lancement du programme, de la remise à zéro de l'unité de traitement, ou encore du temps qui s'est écoulé depuis un événement ou un signal de référence externe ou interne.

Cette possibilité de pouvoir observer le déroulement d'un programme dans un microprocesseur ou un microcalculateur est un inconvénient majeur lorsque ce microprocesseur ou microcalculateur est utilisé dans des application de haute sécurité. En effet, un individu mal intentionné pourrait ainsi connaître les états successifs dans lesquels se trouve le processeur et tirer parti de ces informations pour connaître certains résultats internes de traitement.

On peut imaginer, par exemple, qu'une action donnée sur un signal externe puisse se produire à des instants différents en fonction du résultat d'une opération sécuritaire déterminée, tel que le test d'une information confidentielle interne ou le déchiffrement d'un message, ou encore le contrôle d'intégrité de certaines informations. Selon l'instant considéré, ce signal externe pourrait donner des renseignements sur le résultat ou sur le contenu confidentiel de l'information, et même, dans le cas de calculs cryptographiques, sur la clé secrète de chiffrement utilisée.

Par ailleurs il est connu des microprocesseurs ou microcalculateur tels que ceux commercialisés par la Société SGS Thomson sous la référence ST16XY qui comportent un microprocesseur incorporant un générateur aléatoire dont la lecture permet d'obtenir un nombre aléatoire utilisé, par exemple pour les calculs d'encryptages ou de décryptages.

C'est un des buts de l'invention que de doter le circuit de moyens interdisant le type d'investigation décrit plus haut, et plus généralement d'empêcher les observations illicites ou non du comportement interne du circuit.

Ce but est atteint par le fait que le circuit intégré perfectionné possède des moyens de décorrélation du déroulement d'au moins une séquence d'instruction d'un programme avec les signaux électriques internes ou externes du circuit.

Selon une autre particularité les signaux électriques du circuit sont des signaux de cadencement, de synchronisation ou d'état.

Selon une autre particularité les moyens de décorrelation comprennent un ou plusieurs circuits qui engendrent une succession d'impulsions d'horloge ou de cadencement dont la répartition est aléatoire dans le temps.

Selon une autre particularité les moyens de décorrélation comprennent un générateur aléatoire permettant une désynchronisation de l'exécution de la séquence de programme dans le processeur.

Selon une autre particularité les moyens de décorrélation comprennent un circuit de calibration d'horloge qui permet d'éliminer les impulsions de cadencement trop courtes.

Selon une autre particularité les moyens de décorrelation comprennent un système de génération aléatoire d'interruption.

Selon une autre particularité les moyens de décorrélation comprennent l'exécution de séquences secondaires dont les instructions et temps d'exécution sont différentes et qui sont choisies aléatoirement.

Selon une autre particularité le temps variable du traitement secondaire dépend d'une valeur fournie par un générateur aléatoire.

Selon une autre particularité le traitement secondaire ne modifie pas le contexte général de fonctionnement du programme principal afin de permettre le retour à ce dernier sans avoir à rétablir ce contexte.

Selon une autre particularité le traitement secondaire rétabli le contexte du programme principal avant de lui redonner le contrôle du processeur.

Selon une autre particularité le programme principal peut autoriser ou inhiber un ou plusieurs moyens de décorrélation.

Selon une autre particularité il possède des moyens de déphasage des signaux de cadencement, de synchronisation ou d'état du processeur.

Selon une autre particularité les moyens de déphasage génèrent un déphasage aléatoire des signaux de cadencement, de synchronisation ou d'état du processeur.

Selon une autre particularité les moyens de déphasage aléatoires désynchronisent, de l'horloge externe, le fonctionnement du processeur partiellement ou totalement pendant l'exécution d'un programme.

Selon une autre particularité le générateur aléatoire utilise des compteurs rebouclés ou non et initialisés par une valeur aléatoire.

Selon une autre particularité la valeur d'initialisation provient d'une mémoire non volatile.

Selon une autre particularité la valeur d'initialisation est modifiée pendant l'exécution d'un programme.

Selon une autre particularité le générateur aléatoire utilise un algorithme de type cryptographique ou une fonction de hachage initialisés par la valeur d'initialisation.

Selon une autre particularité le séquencement des actions tient compte des temps nécessaires pour accéder aux divers registres, aux mémoires et aux organes internes, mais aussi et surtout des temps de propagation

des signaux sur les bus et à travers les divers circuits logiques.

Un autre but de l'invention est de proposer un procédé d'utilisation du circuit intégré.

Ce but est atteint par le fait que le procédé d'utilisation d'un circuit intégré consiste :

soit à déclencher le séquencement d'une ou plusieurs instructions ou opérations à l'aide d'une horloge à impulsion aléatoire ;

soit à déclencher de façon aléatoire des séquences d'interruption ;

soit à déclencher le traitement d'une séquence aléatoire d'instruction ou d'opération au cours de l'exécution d'une séquence principale d'instruction ou d'opération ;

soit à combiner au moins deux des possibilités ci-dessus.

D'autres particularités et avantages de la présente invention apparaîtront plus clairement à la lecture de la description ci-après faite en référence aux dessins annexés dans lesquels :

la figure 1 représente le schéma de principe des circuits électroniques d'un premier mode de réalisation de l'invention ;

la figure 2 représente une deuxième variante simplifiée de réalisation de l'invention ;

la figure 3A représente le schéma de réalisation du circuit calibrateur ;

la figure 3B représente les schémas de séquencement logiques du circuit calibrateur ;

la figure 4A représente le schéma des circuits logiques de réalisation d'un circuit de déphasage ;

la figure 4B représente le schéma des séquences des signaux de ce circuit ;

la figure 5 représente une troisième variante de réalisation de l'invention ;

la figure 6 représente le schéma des circuits logiques de réalisation d'une horloge interne ;

la figure 7A représente le schéma logique de réalisation du générateur aléatoire ;

la figure 7B représente le schéma logique de réalisation de chaque cellule du générateur aléatoire.

la figure 8 représente de façon schématique un exemple de séquences du programme secondaire choisies aléatoirement.

Dans la description, on entend par microcalculateur un circuit intégré monolithique incorporant un microprocesseur avec sa mémoire vive de type RAM associée à au moins une mémoire non volatile programmable ou non telle que, par exemple, de type RAM avec alimentation de sauvegarde, ou ROM, ou PROM, ou EPROM, ou EEPROM etc...ou une combinaison de ces mémoires. L'invention va maintenant être explicitée à l'aide de la figure 1 dans laquelle un CPU (1) comporte un générateur aléatoire (2) qui peut fonctionner sur une horloge interne (11). De tels processeurs sont comme on l'a déjà dit, connus notamment par la famille de microcalculateurs ST16XY. Toutefois, ces microcalculateurs ou microprocesseurs qui utilisent un registre à décalage à entrées-sorties parallèles rebouclé sur au moins une de ses entrées et dont le décalage est cadencé par une horloge interne pour constituer le générateur aléatoire, se servent de l'horloge externe de séquencement des cycles machines du microprocesseur, pour exécuter l'instruction de lecture du contenu du registre. Ceci permet de générer un nombre aléatoire et non pas pseudo aléatoire en se basant sur le fait que l'horloge interne du générateur aléatoire, qui a une fréquence multiple de l'horloge externe, est déphasée aléatoirement par rapport à celle-ci.

L'invention consiste à utiliser le principe d'un tel microprocesseur à générateur aléatoire en lui adjoignant un certain nombre d'éléments qui vont

permettre au microprocesseur exécutant le programme principal de passer d'un fonctionnement parfaitement en phase et corrélé à l'horloge externe de séquencement à un fonctionnement décorrélé, dans lequel, au choix et selon le mode de réalisation sélectionné, le temps d'exécution d'une instruction déterminée ne sera plus identique, même lorsque la même instruction est exécutée plusieurs fois, ou bien dans lequel la durée d'exécution d'une séquence d'instruction sera variable même si la même séquence est exécutée à plusieurs reprises par le programme principal, ou bien dans lequel la durée d'exécution d'une séquence d'instruction sera variable, le temps d'exécution d'une même instruction étant lui même variable. Ceci est obtenu par le circuit de la figure 1, dans lequel en plus du générateur aléatoire (2), l'horloge interne (11) est réalisée par un oscillateur libre à fréquence constante, désynchronisée et déphasée par rapport à l'horloge externe CLKE du microprocesseur ou microcalculateur. Dans l'art antérieur, l'homme de métier n'envisageait pas de cadencer le fonctionnement d'un microcalculateur ou d'un microprocesseur avec une horloge irrégulière. Au contraire, tout était fait pour que le fonctionnement soit cadencé régulièrement par les signaux d'horloge provenant en général d'un circuit séquenceur qui engendre les impulsions électriques nécessaires, notamment en déphasant les signaux par rapport à l'horloge de référence. Ceci était dû notamment au fait que le séquencement des actions doit tenir compte des temps nécessaires pour accéder aux divers registres, aux mémoires et aux organes internes, mais aussi et surtout des temps de propagation des signaux sur les bus et à travers les divers circuits logiques. Dans l'invention, le générateur aléatoire (2) est utilisé, soit pour fournir une valeur aléatoire aux divers organes par l'intermédiaire du bus de donnée (3) et la charger dans les différents éléments que nous décrirons ci-après, soit

pour générer un signal impulsionnel de périodicité variable sur sa sortie (22). Dans un microprocesseur ou microcalculateur de l'invention, les signaux nécessaires au chargement et à l'exécution des instructions peuvent donc être engendrés à partir d'impulsion d'horloge répartie de façon aléatoire, mais ces impulsions doivent respecter un temps de cycle minimal afin que le processeur (1) ait un délai suffisant pour l'exécution de diverses opérations. Ce signal, pour servir d'horloge au microprocesseur (1), doit être envoyé sur un circuit calibrateur (9). La sortie (95) de ce circuit calibrateur est envoyée sur un circuit de multiplexage (18) dont l'entrée (19) de commande du multiplexage reçoit le signal d'un ou plusieurs bits d'un registre (8) qui peut être chargé soit par le générateur aléatoire (2), soit par une valeur déterminée par le programme principal (5). Lorsque ce registre (8) est chargé avec une valeur aléatoire, la décision de sélection du signal d'horloge envoyée sur le processeur est faite aléatoirement, tandis que lorsque ce registre (8) est chargé par une valeur déterminée par le programme principal, c'est le programme principal qui va choisir si l'horloge de séquencement du microprocesseur sera l'horloge externe CLKE ou une horloge de décorrélation CLK2. De même, un ou plusieurs bits du registre (8) sont envoyés par la liaison (82) à un circuit logique (28) qui permet en fonction du ou des bits du registre (8), de valider ou non la transmission du signal d'horloge interne (11) au générateur aléatoire (2). Ce générateur aléatoire peut donc fonctionner sur l'horloge externe CLKE en recevant son signal par la liaison (26) et le circuit logique (28). Dans ce dernier cas, les valeurs générées seront des valeurs pseudo aléatoires. Le générateur aléatoire (2) peut fonctionner en utilisant l'horloge interne (11) validée à travers le circuit (28) par le ou les bits du registre (8) et, dans ce cas, les valeurs générées seront des valeurs

aléatoires. Le signal I généré en sortie du générateur aléatoire (2) et reçu par le circuit calibrateur (9) correspond à un signal impulsionnel dont la périodicité varie, soit aléatoirement, soit de façon pseudo-aléatoire. Le fait que cette périodicité varie de façon pseudo aléatoire est peu gênant car, comme on le verra par la suite, le circuit de calibration (9) fait intervenir un signal d'horloge interne (FRC) qui lui-même va réintroduire une décorrélation, par une fréquence différente et un déphasage par rapport au signal d'horloge externe CLKE et par conséquent par rapport au signal d'horloge pseudo-aléatoire synchronisé sur ce signal d'horloge externe.

Le dispositif comprend également un registre R2 qui est chargé, soit par le générateur aléatoire (2) à l'aide d'un nombre aléatoire, soit par le programme principal (5) avec une valeur déterminée par le programme; Ce registre R2 est utilisé en totalité ou en partie par un circuit logique (4) de déclenchement d'une interruption qui reçoit sur une de ses entrées le signal d'horloge décorrélé CLK2 provenant de la sortie (95) du circuit calibrateur (9). La sortie du circuit (4) est envoyée à travers une porte (48) commandée par un plusieurs bits du registre (8) sur l'entrée (12) d'interruption du CPU. Le ou les bits de ce registre (8) jouent le rôle de commande de masquage de l'interruption que l'on trouve de façon classique sur certains microprocesseurs. Lorsqu'une interruption est présentée sur l'entrée (12) d'interruption du processeur, le programme de traitement de l'interruption contenu, par exemple, dans le système d'exploitation (50) va introduire un temps de traitement différent pour la séquence interrompue du programme principal.

Enfin, le dispositif de l'invention comprend d également un programme secondaire (6) qui peut, comme on le verra par la suite, générer un temps de durée variable

qui varie à chaque fois que ce programme secondaire (6) est appelé par le programme principal (5). Ainsi, la variante de réalisation représentée à la figure 1 permet au programme principal (5) de faire évoluer les degrés de protection souhaités, soit en déclenchant le séquencement d'exécution d'une ou plusieurs instructions à l'aide de l'horloge décorrélée CLK2, soit en décidant au cours de l'exécution d'une séquence d'instruction d'introduire ou non une gestion d'interruption déclenchée aléatoirement, soit encore en décidant ou non, au cours de l'exécution de la séquence, d'introduire un saut vers le programme secondaire (6) qui génère également un traitement de temps variable, ou encore en combinant ces différentes possibilités. Ainsi, ce programme secondaire (6) peut, dans une variante de l'invention, être constitué comme représenté à la figure 8 par une pluralité de séquences (61, 62, 63...6n) qui seront appelées de façon aléatoire; et chaque séquence (0, 1, 2 ou 2^{n-1}) mettra en oeuvre un ensemble d'instructions différentes qui entraîneront un temps de traitement variable dans chaque branche et des comportements différents du microprocesseur. Les séquences pourront être appelées de façon aléatoire ; par exemple, après que le programme principal ait effectué le saut au programme secondaire, ce dernier charge, aux étapes (64 et 65), une valeur aléatoire V provenant de la mémoire (7) dans deux registres, par exemple R10 et R11 du microprocesseur (1). Le programme secondaire incrémente cette valeur V, puis le programme commande la mémorisation de cette valeur incrémentée dans la mémoire non volatile (7) à l'étape 66. Cette valeur, mémorisée dans la mémoire non volatile (7), est destinée à une utilisation ultérieure. Le programme secondaire, à l'étape 67, prélève ensuite n bits de poids forts ou faibles dans R10 afin d'obtenir une valeur r qui permettra de désigner la séquence de programme à exécuter parmi les séquences (61, 62, 63,....., 6n) de programme

secondaire (6). Chaque séquence de programme secondaire produira un traitement différent : par exemple, la séquence (0) consiste d'abord, à l'étape 611, à transférer le contenu du registre R11 du microprocesseur dans un registre R12. A l'étape 612, le contenu de R12 est additionné avec la valeur de retenue (CARRY), puis à l'étape 613, un OU exclusif est effectué entre le contenu du registre R11 et le contenu du registre R12 et le résultat est placé dans le registre R12. A l'étape 614, le processeur décrémente R12 ; à l'étape 615, le test est effectué sur la valeur de R12 pour déterminer si R12 est égal à zéro. Dans le cas où R12 = 0, le processeur retourne à l'exécution du programme principal. Dans le cas contraire, à l'étape 616, le programme secondaire (61) effectue une rotation du contenu du registre R10. L'étape suivante consiste à extraire n bits de poids déterminé du registre R10, pour ensuite accéder à l'une des séquences déterminées par cette valeur r dans le programme secondaire. On pourra ainsi accéder par exemple à la séquence (2^{n-1}) qui consiste, à l'étape (6n1), à transférer le résultat de la multiplication des valeurs de R10 et de R11 dans R13 et R14. A l'étape (6n2), cette séquence effectue une rotation de R13 et R14, puis, à l'étape (6n3), le contenu de R13 est transféré dans R11. A l'étape (6n4), R11 est décrémenté pour ensuite, à l'étape (6n5), effectuer un test sur la valeur R11. Ce test consiste à déterminer si le contenu de R11 = 3. Dans l'affirmative, on retourne au programme principal et dans la négative le programme se poursuit à l'étape (6n6) par une rotation à gauche de R10, puis par l'exécution de l'instruction (67) pour accéder à une nouvelle séquence de programme secondaire.

Dans le cas où est envisagée une combinaison du programme secondaire avec une horloge décorrélée ou des gestions d'interruption, il est possible, dans une telle combinaison de se contenter d'un programme secondaire

produisant un traitement plus simple. Un tel programme secondaire simplifié peut être constitué des instructions ci-après :

MOV B, R2 qui consiste à charger le registre R2 dans le registre B microprocesseur

LOOP

DCX B qui consiste à décrémenter le registre B de la valeur A

JNZ B LOOP qui consiste à faire un test sur la valeur du registre B et à reboucler sur l'étiquette LOOP dans le cas où cette valeur est différente de zéro.

Cette séquence se termine par une instruction de retour à l'instruction du programme principal qui était immédiatement après la dernière instruction exécutée avant le saut au programme secondaire (6). Le registre R2 est préalablement chargé par une instruction du programme principal (5) avant le saut au programme secondaire (6) avec une valeur aléatoire fournie par le générateur aléatoire (2). Ainsi, l'exécution du programme secondaire ci-dessus défini générera toujours une durée variable.

Un autre mode de réalisation d'un programme secondaire de durée variable peut consister à définir une zone de la mémoire programme correspondant au programme secondaire (6) dans laquelle une série d'instructions est mémorisée. De préférence, on choisit des instructions nécessitant des nombres de cycles machines différents pour s'exécuter, comme cela est connu par exemple, avec les instructions J, CALL, RET, RST, PCHL, INX, par rapport à des instructions nécessitant un nombre de cycles machines plus courts comme ADC, SUB, ANA, MOV etc... Dans cette zone mémoire, on dispose donc d'un certain nombre d'instructions ayant les unes par rapport aux autres des durées d'exécution différentes en nombre de cycles machines. Le programme principal (5) comporte une instruction de saut à une adresse indexée dont

l'index correspond au contenu du registre R2 et l'adresse correspond à la première adresse de la zone (6). L'exécution de cette instruction du programme principal (5) fait donc adresser par le processeur (1), de façon aléatoire, des instructions dont les durées d'exécution seront différentes selon la position adressée. De façon connue, le générateur aléatoire (2) sera initialisé au départ par une variable. Cette variable initiale est contenue dans une mémoire non volatile (7) et constituée, par exemple par la dernière valeur aléatoire générée par le générateur (2) avant l'arrêt du microprocesseur (1).

La figure 2 représente une autre variante de réalisation simplifiée de l'invention, dans laquelle le contenu du registre (8) va commander le multiplexeur (18) pour décider si l'horloge externe CLKE est envoyée sur le processeur (1) ou bien si simplement l'horloge décorrélée CLK2 est utilisée par le CPU (1). Ce registre (8) est chargé par le bus (30) sur exécution d'une instruction du programme principal (5) qui aura été conçu pour décider à un moment donné de déclencher le mode sécuritaire en générant des séquences d'exécution d'instructions de durée variable. Le générateur aléatoire (2) est en communication par un bus (31) avec la mémoire non volatile (7) qui permet, par exemple, la mémorisation de la dernière valeur générée pour que, lors d'une nouvelle connexion du circuit monolithique, le générateur aléatoire soit réinitialisé avec une valeur différente de la précédente valeur initiale. Ce bus (31) est éventuellement contrôlé par le processeur (1). Dans une autre variante, l'inscription dans la mémoire (7) peut être contrôlée par une logique câblée.

Dans un autre mode de réalisation, il est possible d'introduire un circuit (45) de déphasage variable à la sortie du circuit d'horloge, comme le montre la figure 4, ce circuit de déphasage étant par exemple constitué par un registre à décalage D1 à D5 cadencé par le signal FRC

provenant du circuit (11), ou FRC recalibré fourni par la sortie (95) du circuit (9), et déphasant le signal I fourni par la sortie (22), qui peut être divisé par un facteur de ralentissement dans un diviseur (452). La sortie du circuit de déphasage (45) peut être réalisée à l'aide d'un multiplexeur (451) MUX qui permet de prélever l'un quelconque des signaux de sortie Q1, Q2, ... Q5, du registre à décalage en fonction du contenu du registre RM qui est chargé, soit directement par le générateur aléatoire (2), soit indirectement par le programme principal (5), ou même par le programme secondaire (6) à travers le bus (3). Dans ce cas, les fronts d'horloge S délivrés en sortie peuvent être retardés ou avancés, par rapport à une impulsion médiane fournie par l'étage central du registre à décalage, d'une valeur qui dépend d'un nombre aléatoire, retardant ou avançant d'autant le séquencement d'exécution des instructions du programme en cours.

Dans un autre mode de réalisation, le générateur aléatoire et le circuit de déphasage peuvent être mis en oeuvre en permanence pendant certaines périodes particulièrement sensibles; pendant ces phases, le processeur est cadencé de façon complètement aléatoire, puisque les intervalles de temps qui séparent les impulsions d'horloge sont variables, et non pas constants comme c'est le cas dans les processeurs classiques.

L'organisation des programmes exécutés par le processeur peut être réalisée de telle manière que le fonctionnement du processeur (1) soit piloté par un véritable système d'exploitation sécuritaire qui décide du type de brouillage à mettre en oeuvre en fonction du type de programme exécuté par la machine. Dans ce cas c'est le système d'exploitation qui gère comme bon lui semble les divers signaux provenant du générateur aléatoire, du calibrateur, des interruptions ou des commandes du circuit de déphasage et du lancement des

programmes principal et secondaire. Il est clair que le programme secondaire peut être utilisé pour réaliser d'autres fonctions qu'une simple temporisation, notamment en effectuant des traitements qui peuvent être utiles au programme principal de façon à tirer parti du temps dédié au programme secondaire, ces traitements pouvant être constitués, par exemple, par des préparations de calculs utilisés ultérieurement par le programme principal. Bien entendu, on peut facilement généraliser les mécanismes de l'invention lorsque le processeur fonctionne en multiprogrammation, les programmes d'application pouvant alors être considérés comme autant de programmes principaux. Le générateur aléatoire et le circuit de déphasage d'horloge vus plus haut ne posent pas de problèmes particuliers de réalisation et sont connus de l'homme de l'art lorsqu'ils sont utilisés séparément pour d'autres usages n'ayant aucun lien avec l'invention.

On peut aussi réaliser un cinquième mode de réalisation simplifié de l'invention qui n'utilise pas d'interruption. Lorsque le programme principal veut se protéger, il déclenche lui-même un programme secondaire qui engendre un traitement de longueur aléatoire à des instants choisis par lui, soit au début, soit en cours de traitement, de façon à brouiller les différentes séquences.

Les différents circuits permettant la réalisation de l'invention vont être maintenant explicités en liaison avec les autres figures. Ainsi, un générateur aléatoire représenté sur les figures 7A et 7B est constitué, par exemple, d'un ensemble de cellules (B0 à B7) formées chacune d'une porte (23) OU exclusif à deux entrées, reliée à une bascule (24) de type D dont la sortie (Q) est reliée à une des deux entrées de la porte OU exclusif de la cellule suivante. La deuxième entrée de la porte OU exclusif reçoit le signal d'entrée des données provenant du bus (3) pour permettre le chargement d'initialisation

ou pour les cellules (B0) et (B3), par exemple, un signal de rebouclage (25) provenant de la dernière cellule (B7). La sortie (22) de la dernière cellule (B7) constitue également la sortie qui délivre le signal impulsionnel (I) à périodicité aléatoirement variable. Ce signal (I) est ensuite utilisé dans le circuit calibrateur (9) représenté à la figure 3A. La figure 3B représente le séquencement des signaux d'entrée et de sortie de ce circuit calibrateur (9) de la figure 3A. Ce circuit calibrateur est constitué de deux portes (90, 91) NON ET à trois entrées recevant chacune sur une entrée le signal I provenant de la sortie (22) du générateur aléatoire (2). Une première porte NON ET (91) reçoit la sortie (Q2) d'une bascule (93) de type JK tandis que l'autre porte (90) reçoit la sortie inversée (NQ2) de cette bascule (93). Cette bascule (93) reçoit sur son entrée d'horloge un signal d'horloge FRC qui constitue une horloge interne au circuit. Cette horloge interne est générée par exemple par un circuit représenté à la figure 6. Les entrées J et K de cette bascule (93) sont reliées à la tension d'alimentation représentative du niveau logique (1). Le signal d'horloge interne FRC est envoyé par un circuit inverseur (92) sur chacune des troisièmes entrées des porte NON ET (90, 91). La sortie de la première porte NON ET (90) est envoyée sur l'entrée de mise à 1 de la deuxième bascule logique (94) alors que la sortie de la deuxième porte NON ET (91) est envoyée sur l'entrée de remise à zéro de la deuxième bascule (94). Cette deuxième bascule (94) a son entrée d'horloge et son entrée (J) reliées à la tension d'alimentation représentative du niveau (1) et l'entrée (K) reliée à la tension d'alimentation représentation du niveau zéro. La sortie (Q1) de cette deuxième bascule (94) délivre le signal CLK2 fourni par la liaison (95) au multiplexeur (18). L'horloge interne FRC délivre, sur la liaison (111), des signaux impulsionnels périodiques ayant une largeur

d'impulsion minimale Tm qui est définie par le circuit de la figure 6. Ce circuit (11) est constitué par exemple par une série d'inverseurs (111 à 115), en l'occurrence cinq, qui ont chacun un temps de propagation déterminé, par exemple de 10 nanosecondes, ce qui permet d'obtenir sur la sortie FRC une impulsion de 50 nanosecondes. Cette sortie FRC est rebouclée par la liaison (116) sur l'entrée du premier inverseur (111) et, l'entrée du premier inverseur (111) est également alimentée à travers une résistance (117) par la tension d'alimentation de 5 volts. La largeur d'impulsion est choisie à 50 nanosecondes mais il est bien évident qu'en faisant varier le nombre de portes inverseuses on fait varier la valeur T_m. Cette valeur T_m va être utilisée, comme représenté à la figure 3B, par le circuit logique (9) de la figure 3A pour générer, à partir du signal impulsionnel de périodicité aléatoirement variable (I), un signal impulsionnel CLK2 dont les impulsions de largeur variable ont une valeur minimale T_m et dont la périodicité est également variable et désynchronisée par rapport à l'horloge externe CLKE. En effet, l'horloge interne se mettant à fonctionner dès la mise sous tension du circuit intégré, si la périodicité initiale de cette horloge est différente de la périodicité de l'horloge externe il n'y a aucune chance pour qu'au démarrage les horloges soient synchronisées. Les signaux de ce calibrateur (9) possèdent une période au moins égale à deux fois le temps minimal T_m nécessaire au processeur pour exécuter un cycle interne. Tous les fronts du signal CLK2 seront distants d'au moins la valeur Tm mais leur position et leur durée exacte seront aléatoires.

On voit ainsi que, quelle que soit la variante de réalisation, que le déroulement du programme principal est réalisé selon un séquencement imprévisible qui dépend selon la variante, soit du générateur aléatoire, soit de l'horloge aléatoire, soit du programme secondaire, soit

des interruptions aléatoires, soit d'une combinaison d'au moins deux de ces dispositifs. Lorsque le programme principal exécute des fonctions non sensibles sur le plan sécuritaire, il peut ainsi recourir à l'horloge externe CLKE, par exemple pour délivrer des résultats au monde extérieur ou encore masquer l'interruption de décorrélation de façon à optimiser le temps de traitement. Dès qu'une fonction sécuritaire est mise en oeuvre, le programme principal (5) autorise le fonctionnement en mode aléatoire, soit en validant l'horloge aléatoire, soit l'interruption de décorrélation (ou les deux) afin de "brouiller" les divers signaux de fonctionnement, notamment en désynchronisant l'horloge par rapport au programme principal, soit encore en faisant appel au programme secondaire.

Pour le générateur aléatoire (2), on peut, par exemple, utiliser des compteurs rebouclés ayant des périodes différentes, ces compteurs étant initialisés par une "graine" stockée en mémoire non volatile (7). Lorsque le processeur démarre, les compteurs prennent en compte la valeur stockée comme valeur de départ. En cours de calcul, ou à la fin du calcul, la mémoire non volatile (7) est mise à jour avec une nouvelle valeur qui va servir de graine pour initialiser les compteurs à la prochaine initialisation. Le circuit (4) de génération des interruptions peut être conçu de façon que la génération des impulsions d'interruption vues plus haut puisse, par exemple, se produire lorsque le nombre généré possède certaines caractéristiques telles que l'égalité avec certaines données du programme. Ce circuit (4) peut aussi prendre la valeur d'un ou plusieurs bits d'un ou plusieurs compteurs. Il est également possible de réaliser un très bon générateur aléatoire en utilisant un algorithme cryptographique (69) comme le montre la figure 5 ou une fonction de hachage initialisés par la graine vue plus haut. Dans ce cas, le générateur peut être sous

la forme d'un programme mettant en oeuvre l'algorithme exécuté par le processeur (1) et mettant en oeuvre par exemple l'algorithme cryptographique en recevant d'une part une variable stockée dans la mémoire non volatile (7), d'autre part une clé pour générer un résultat stocké dans un registre tampon (41). Ce résultat stocké dans le registre tampon est ensuite traité par un dispositif décodeur (42) logiciel ou matériel pour générer soit le signal d'horloge décorrélée CLK2, soit un signal d'interruption pour le processeur (1). On voit facilement que ce générateur de nombre aléatoire peut être également utilisé pour engendrer les divers nombres aléatoires vus plus haut. Une autre manière de réaliser un tel générateur est d'amplifier la tension engendrée aux bornes d'une diode dite "de bruit" et de mettre en forme les signaux après un filtrage passe bas pour éviter que les impulsions de bruit trop rapide ne perturbent le fonctionnement.

Pour le circuit de déphasage d'horloge, il existe d'autres possibilités que celle vue plus haut. Par exemple un registre à décalage piloté par une horloge 10 fois plus élevée que celle du processeur. Si l'on suppose que le registre comporte dix bascules, on dispose de dix impulsions ayant des phases différentes qui peuvent être choisies par le processeur à l'aide d'un multiplexeur à dix entrées et une sortie. La sortie du multiplexeur est utilisée comme précédemment pour donner le signal d'horloge interne du processeur.

Un autre mode de réalisation consiste à utiliser un circuit du même type que le générateur aléatoire vu plus haut, et de prélever des impulsions sur les différents étages des compteurs. Dans ce cas, le processeur est vraiment cadencé par des impulsions réparties aléatoirement dans le temps.

Un autre mode de réalisation consiste à utiliser les signaux du générateur aléatoire pour prélever les

impulsions du registre à décalage. De très nombreuses combinaisons sont possibles pour sophistiquer les mécanismes, mais les principes de l'invention restent toujours valables.

La variante de réalisation de la figure 1 est la plus complète ; bien évidemment, le circuit monolithique de type microprocesseur ou de type microcalculateur pourra incorporer seulement un, ou plusieurs, ou une combinaison quelconque, des éléments représentés.

Ainsi, selon une variante, le circuit monolithique peut incorporer un microprocesseur, le générateur aléatoire, l'horloge interne (FRC) et le circuit calibrateur formant l'horloge décorrélée.

Dans une autre variante, le circuit monolithique peut incorporer le microprocesseur, le générateur aléatoire, le circuit de génération d'interruption.

Dans une autre variante, le circuit monolithique peut incorporer le microprocesseur, le programme secondaire et les circuits d'horloge décorrélée et calibrée.

Dans une autre variante, le circuit monolithique peut incorporer un microprocesseur, le circuit d'horloge décorrélée et calibrée, et le circuit d'interruption.

Dans d'autres variantes du circuit monolithique, le microprocesseur est remplacé par un microcalculateur.

Dans d'autres variantes du circuit intégré monolithique, le microprocesseur peut être remplacé par une logique combinatoire permettant d'exécuter un nombre d'instructions limitées pour des applications spécifiques. Il est bien évident que dans un tel cas les mêmes mécanismes de sécurisation peuvent être appliqués au circuit intégré.

D'autres modifications à la portée de l'homme de métier font également partie de l'esprit de l'invention.

REVENDICATIONS

1. Circuit intégré perfectionné caractérisé en ce qu'il possède des moyens de décorrélation (6, 2, 9, 18, 40) du déroulement d'au moins une séquence d'instruction d'un programme (5) avec les signaux électriques internes ou externes du circuit intégré (1).

2. Circuit intégré selon la revendication 1, caractérisé en ce que les signaux électriques du microprocesseur ou microcalculateur (1) sont des signaux de cadencement, de synchronisation ou d'état.

3. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que les moyens de décorrélation comprennent un ou plusieurs circuits (18, 9, 8, 28, 11, 2) qui engendrent une succession d'impulsions d'horloge ou de cadencement dont la répartition est aléatoire dans le temps.

4. Circuit intégré selon une des revendications 1 à 3, caractérisé en ce que les moyens de décorrélation comprennent un générateur aléatoire (2) permettant une désynchronisation de l'exécution de la séquence de programme (5) dans le processeur (1).

5. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que les moyens de décorrélation comprennent un circuit (9) de calibration d'horloge qui permet d'éliminer les impulsions de cadencement trop courtes.

6. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que les moyens de décorrelation comprennent un système de génération aléatoire d'interruption (40, 48).

7. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que les moyens de décorrélation comprennent l'exécution de séquences secondaires (6) dont les instructions et temps

d'exécution sont différentes et qui sont choisies aléatoirement.

8. Circuit intégré selon la revendication 7, caractérisé en ce que le temps variable du traitement secondaire dépend d'une valeur fournie par un générateur aléatoire (2).

9. Circuit intégré selon l'une des revendications 7 à 8, caractérisé en ce que le traitement secondaire (6) ne modifie pas le contexte général de fonctionnement du programme principal (5) afin de permettre le retour à ce dernier sans avoir à rétablir ce contexte.

10. Circuit intégré selon l'une des revendications 7 à 9, caractérisé en ce que le traitement secondaire (6) rétabli le contexte du programme principal (5) avant de lui redonner le contrôle du processeur.

11. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que le programme principal (5) peut autoriser ou inhiber (8, R2, 48) un ou plusieurs moyens de décorrélation.

12. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce qu'il possède des moyens (45) de déphasage des signaux de cadencement, de synchronisation ou d'état du processeur.

13. Circuit intégré selon la revendication 12, caractérisé en ce que les moyens de déphasage génèrent un déphasage aléatoire des signaux de cadencement, de synchronisation ou d'état du processeur.

14. Circuit intégré selon la revendication 13, caractérisé en ce que les moyens de déphasage aléatoires désynchronisent, de l'horloge externe, le fonctionnement du processeur (1) partiellement ou totalement pendant l'exécution d'un programme.

15. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que le générateur aléatoire (2) utilise des compteurs rebouclés (B0 à B7) ou non et initialisés par une valeur aléatoire (7).

16. Circuit intégré selon la revendication 15, caractérisé en ce que la valeur d'initialisation provient d'une mémoire non volatile (7).

17. Circuit intégré selon la revendication 16, caractérisé en ce que la valeur d'initialisation est modifiée pendant l'exécution d'un programme.

18. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que le générateur aléatoire utilise un algorithme de type cryptographique ou une fonction de hachage initialisés par la valeur d'initialisation.

19. Circuit intégré selon l'une des revendications précédentes, caractérisé en ce que le séquencement des actions tient compte des temps nécessaires pour accéder aux divers registres, aux mémoires et aux organes internes, mais aussi et surtout des temps de propagation des signaux sur les bus et à travers les divers circuits logiques.

20. Procédé d'utilisation d'un circuit intégré selon une des revendications précédentes caractérisé en ce qu'il consiste :

soit à déclencher le séquencement d'une ou plusieurs instructions ou opérations à l'aide d'une horloge à impulsion aléatoire (CLK2) ;

soit à déclencher de façon aléatoire des séquences d'interruption (40) ;

soit à déclencher le traitement d'une séquence aléatoire d'instructions (6) ou d'opérations au cours de l'exécution d'une séquence principale (5) d'instructions ou d'opérations ;

soit à combiner au moins deux des possibilités ci-dessus.

1/6

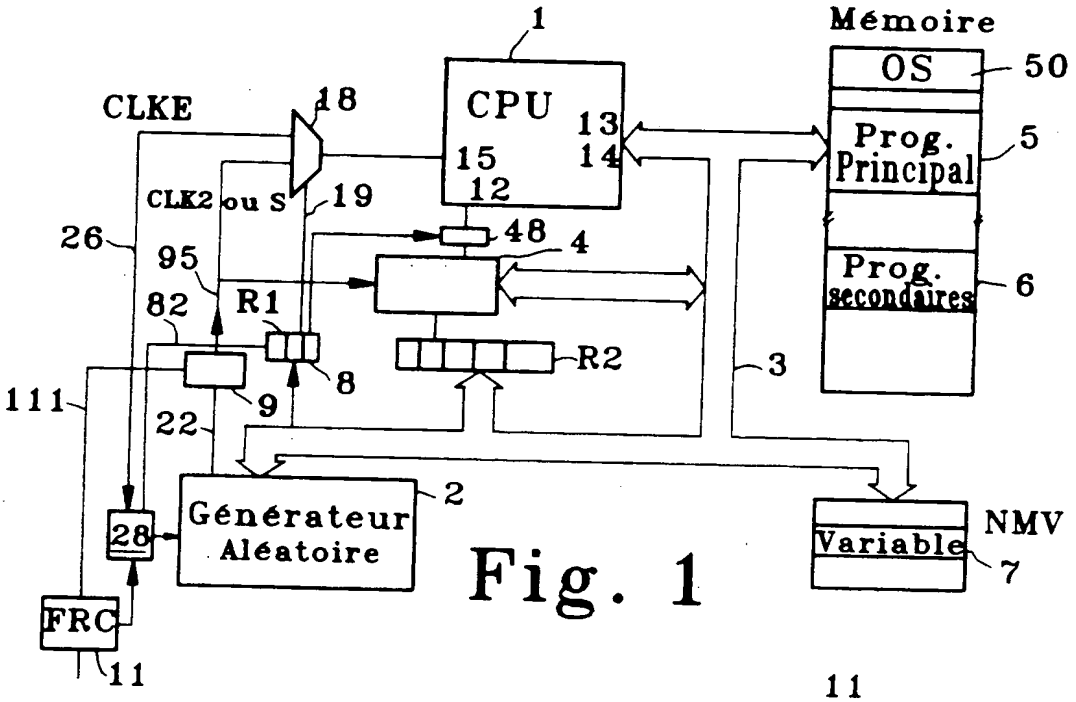
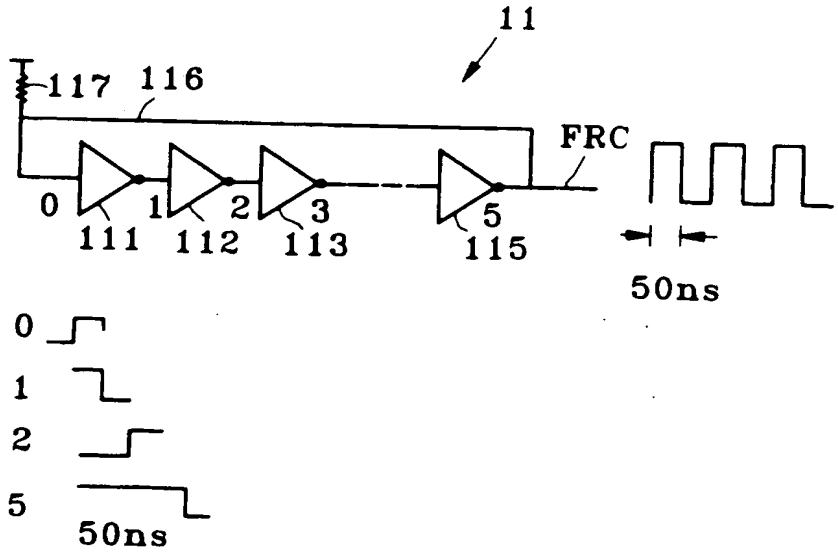


Fig. 1

Fig. 6



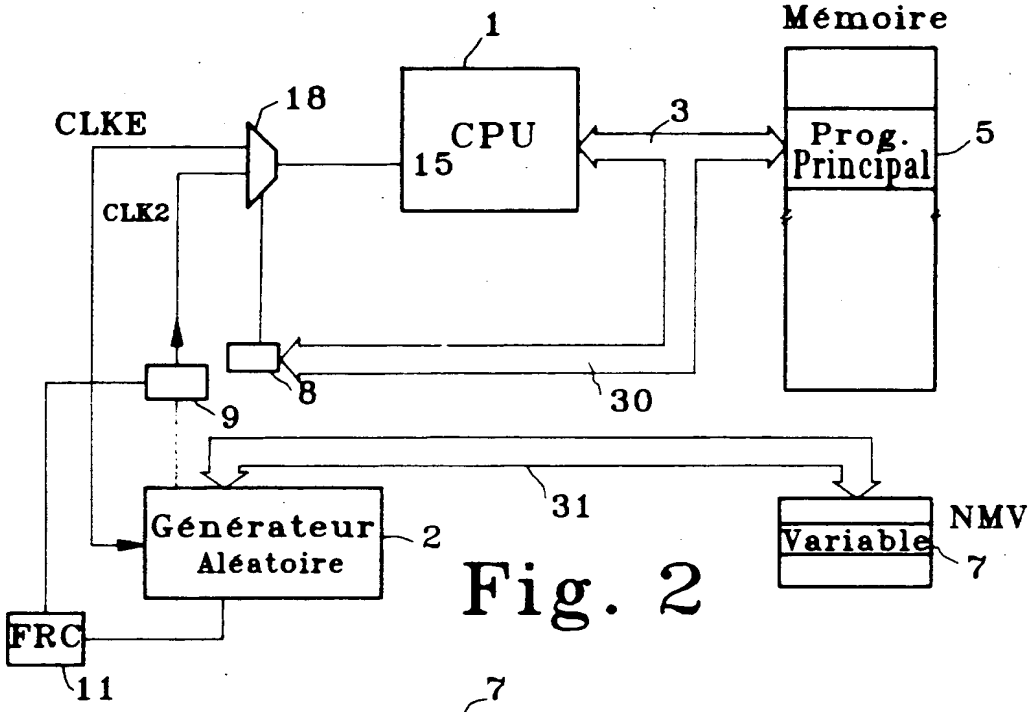


Fig. 2

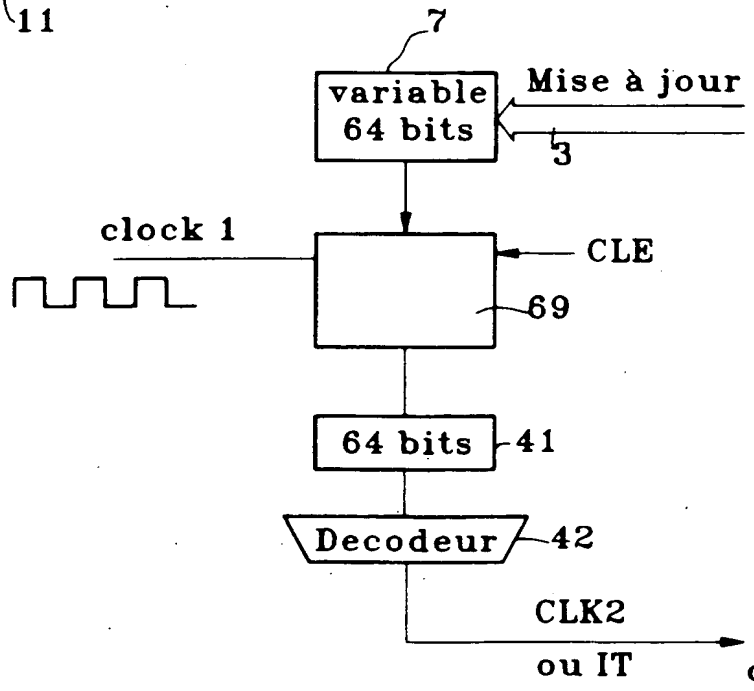
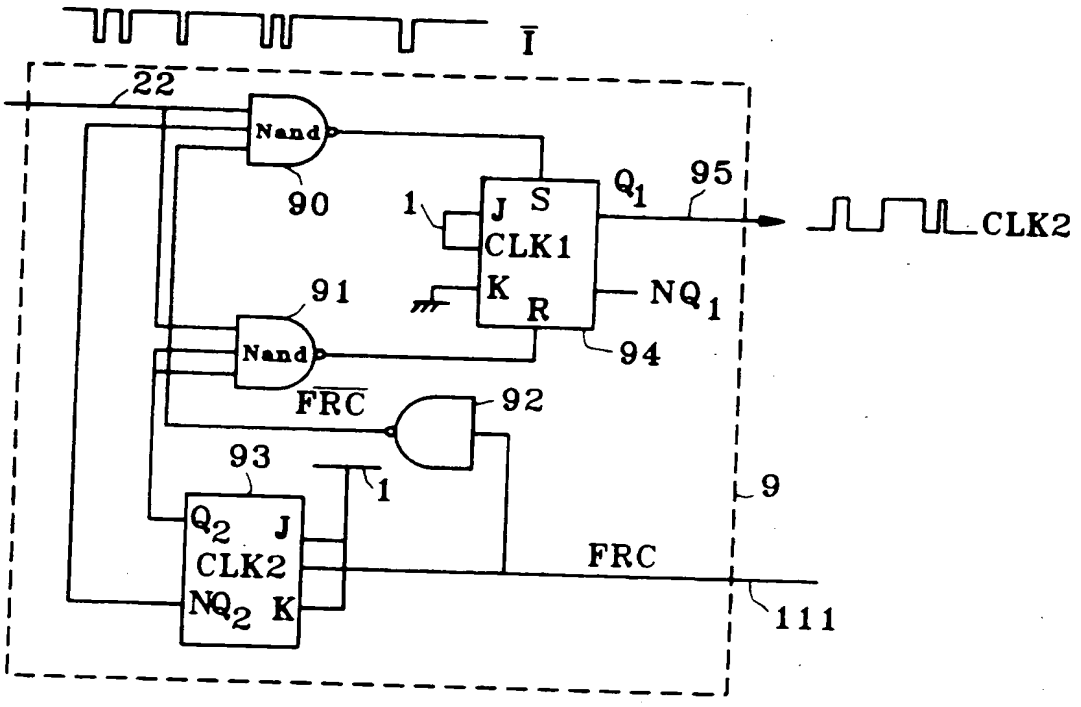


Fig. 5

Fig. 3A



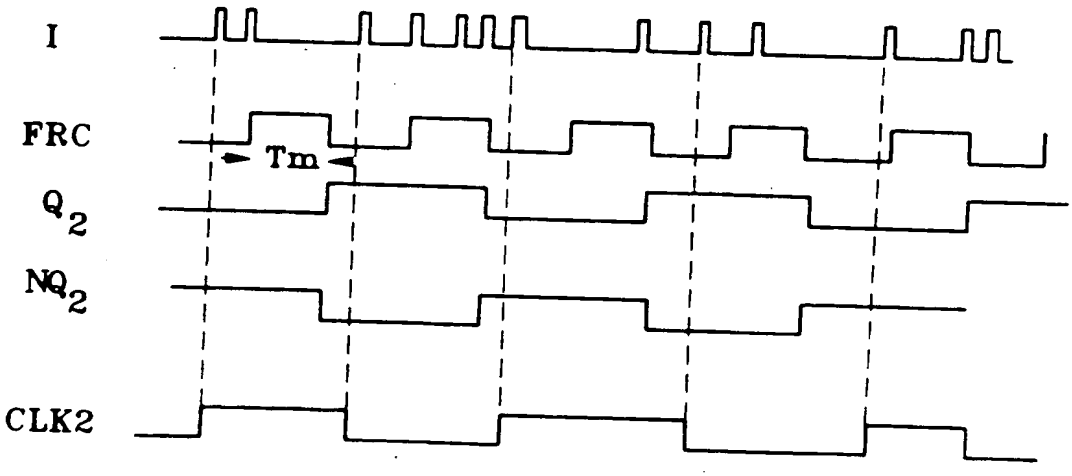


Fig. 3B

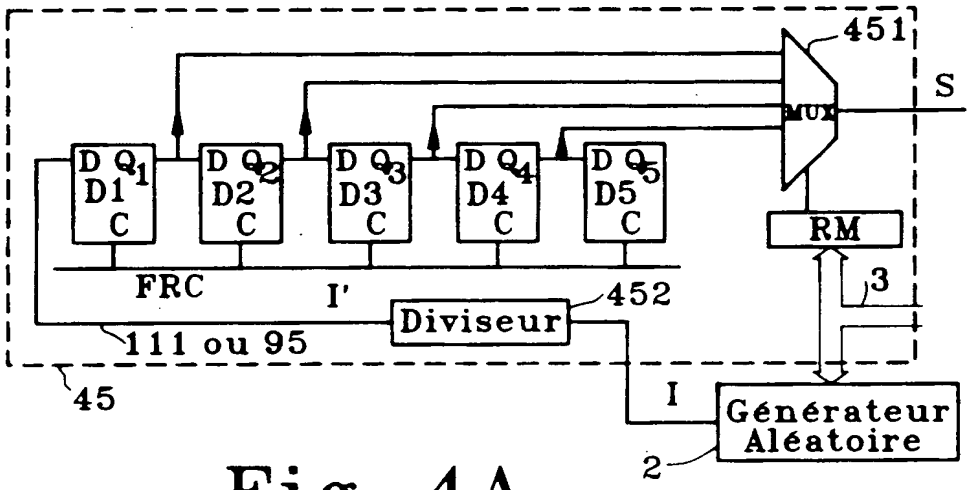


Fig. 4A

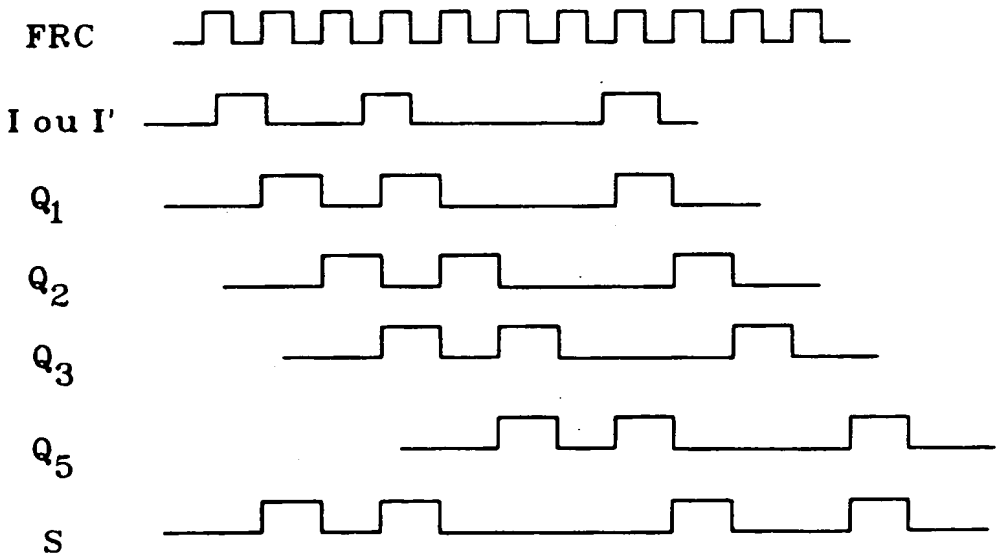
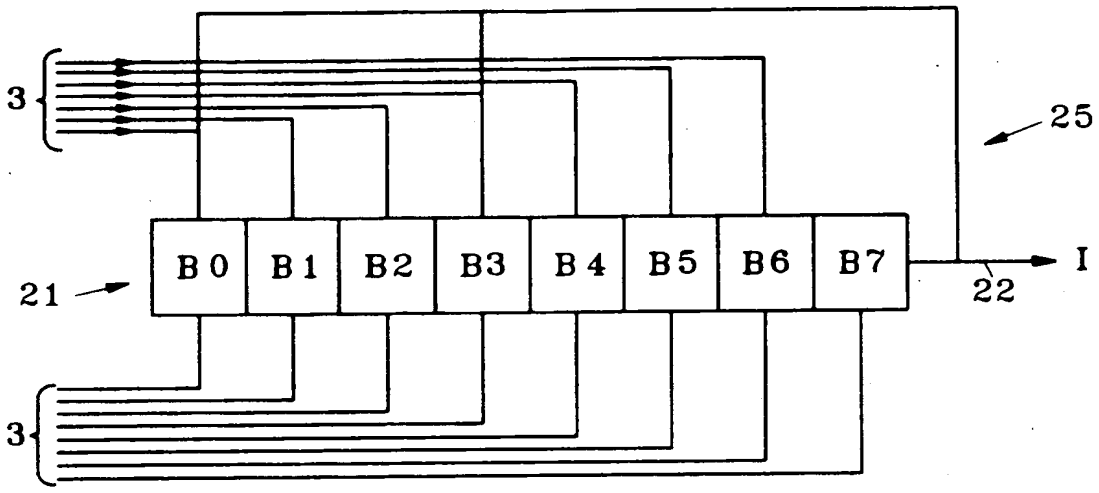


Fig. 4B

Fig. 7A



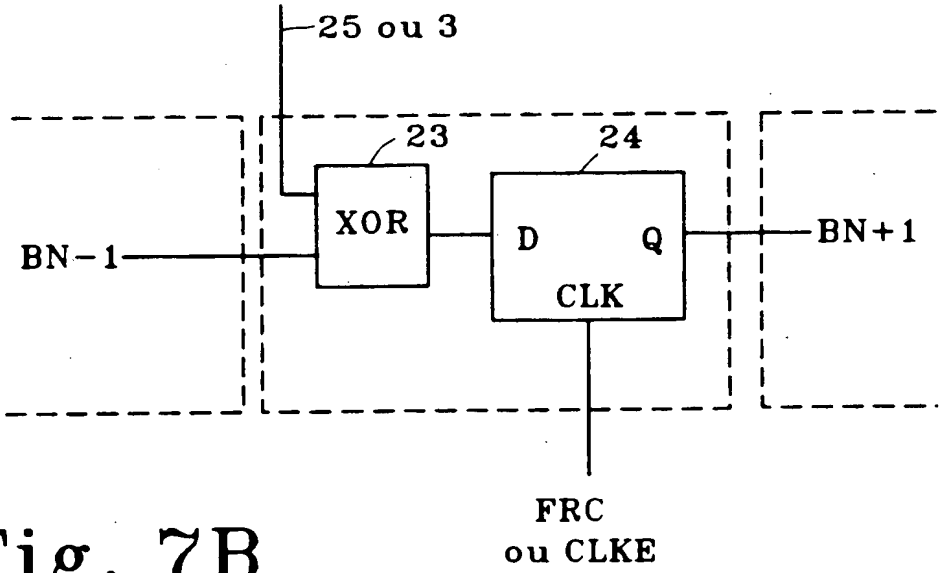


Fig. 7B

Exemple de Programme Secondaire

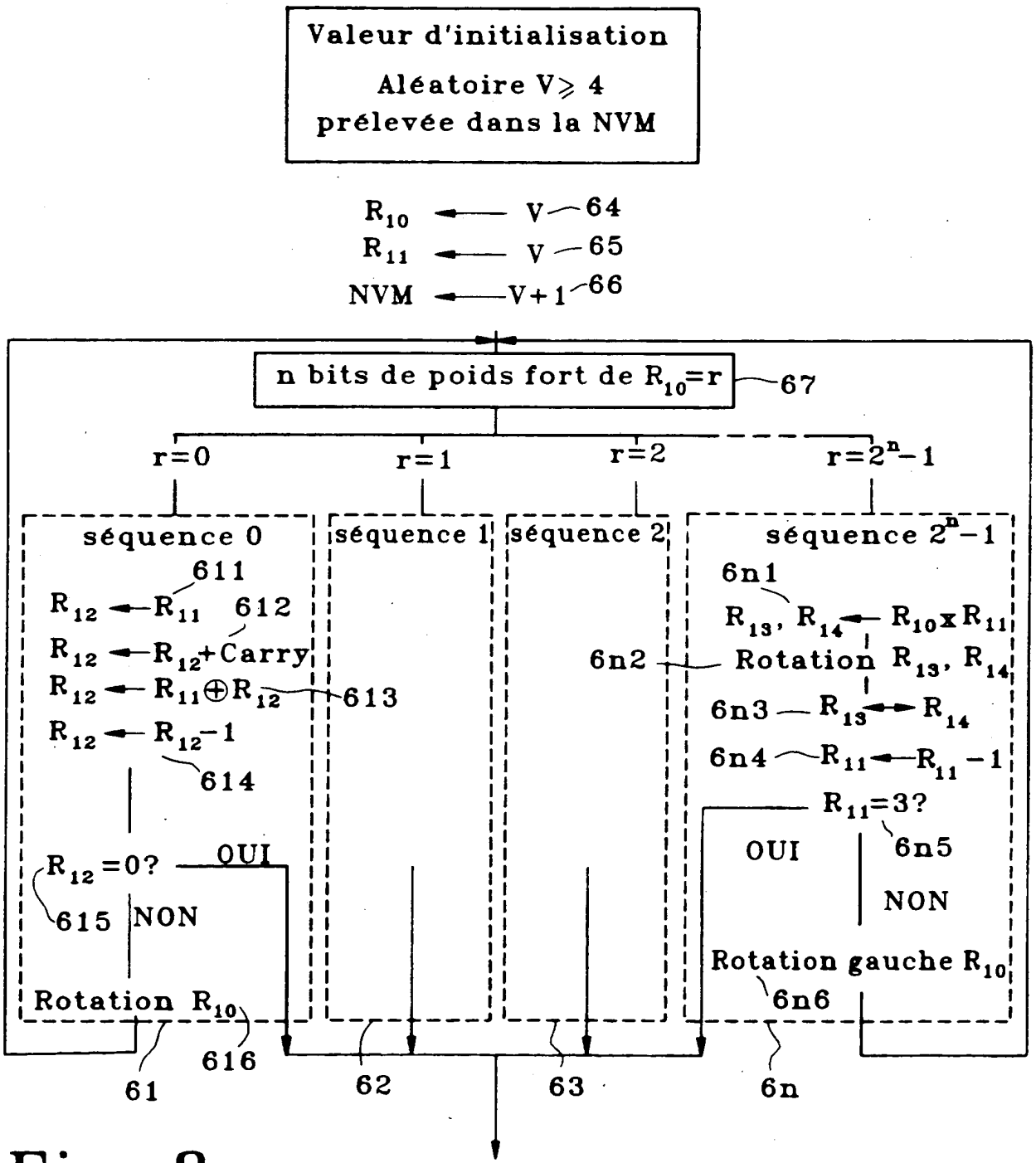


Fig. 8 Retour au programme principal

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2745924
N° d'enregistrement national

FA 530232
FR 9602903

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	US-A-5 404 402 (SPRUNK ERIC) 4 Avril 1995 * abrégé; revendication 1; figures * * colonne 4, ligne 36 - ligne 53 * * colonne 7, ligne 4 - ligne 20 * ---	1-5, 12-18
X	EP-A-0 448 262 (GEN INSTRUMENT CORP) 25 Septembre 1991 * abrégé * * colonne 10, ligne 34-45 * ---	1,2,4, 7-10
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 37, no. 5, 1 Mai 1994, pages 419-421, XP000453206 "ACTIVELY SLOWING A CPU IN RESPONSE TO THE DETECTION OF A SIGNATURE STRING" * page 421, ligne 22 - ligne 23 * -----	6

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G06F

Date d'achèvement de la recherche: 18 Novembre 1996

Examinateur: Durand, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C13)

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)